ABSTRACT

A method for using a device that incorporates a magnetic stripe card reader head with a smart chip and can be connected to a computer network such as the Internet to authenticate a user to a remote server on the network. The method involves reading data from the magnetic stripe (101), verifying data from the magnetic stripe (102), receiving a personal identification number entered on a keyboard on the device (103), verifying the personal identification number (104), encrypting with a key contained in the smart chip a piece of data for sending to the remote server along with information identifying the source (106), and, on the remote server, looking up an appropriate key for decryption based on the identification of the source and verifying the authentication if the decryption is successful (108). Variations on the method include verifying the mag-stripe data on a remote server instead of within the smart chip, verifying the PIN on a remote server instead of within the smart chip, and adding various kinds of information to be sent to the server along with the essential elements required for authentication. The method may be used to authenticate digital signatures or signature guarantees, or for transactions using debit cards or credit cards. If the reader device with a smart chip is owned by a merchant, the merchant can further authenticate himself with a personal identification number, and the card holder will swipe his card into the device and identify himself with a second personal identification number.